REMARKS

With this amendment the independent claims 1, 14 and 15 have been amended. Claims 1-8 and 14-19 are pending.

The Rejection – FINAL.

The last rejection was solely an obviousness rejection.

The Examiner asserts claims 1, 2, 5, 7-8, 14-16 and 19 are obvious in view of Hasu (6,041,410), Flick (6,140,939 and Waraksa (5,412,379).

The rejection of dependent claims 3 and 17 added Nicholls (for the teaching of an electroluminescent fingerprint sensor).

The rejection of dependent claims 4 and 18 added Toyoda (for the teaching of charged coupled devices or CCDs).

The rejection of claim 6 added Fitzgibbon (5,751,224 for the teaching of a wall controller).

The Problem.

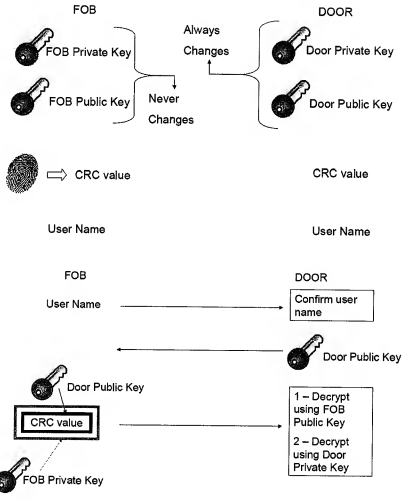
In the past, wireless security systems were vulnerable to code grabbers which would read and store codes from a transmitter being used to gain access to a secured area. Because of that problem, rolling code which changes the access code with each use of that code to gain access to a secured area has been used to defeat code grabbing. Transmitters using rolling code, however, can be lost or stolen. This also compromises security. Transmitters or security systems which relied solely on biometric data, such as finger prints, were thought nearly invulnerable. See Declaration of Fitzgibbon attached to the last amendment. That was not true as will be explained in more detail below. The claims herein describe a barrier operator system and method which address and ***inexpensively*** solve this security problem by combining the use of rolling code which is known with finger print identification technology which is also known. Applicants' barrier movement operator does not require a transmitter which transmits

encrypted signals. Nor does applicants' transmitter outside a secured area require a receiver. Rather, as described in the claims, only the transmitter transmits a changing code which authorizes movement of the barrier. A receiver at the transmitter is not needed. Rolling code and code representative of an authorized user's finger print are combined and transmitted as a changing authorization code without (1) double encryption and (2) without the barrier movement operator being required to transmit to the transmitter a changing door "private key." The changing combined authorization code provides inexpensive security for finger print biometric data and is provides a unique combination which solves the vulnerability of both biometric and rolling code technologies to enhance security.

The References

Hsu

Hsu only involves transmissions indicating valid fingerprints using a double encryption method as described by Hsu at column 6, line 42 through column 7, line 34. In this method the fob has private and public keys and the door has private and public keys. The keys for the fob never change. Hsu at column 7, line 4. The keys for the door always change with a transmission. Hsu at column 7, lines 13-16. The finger print is sensed at the fob and the finger print code, which Hsu calls "CRC", is read into the transmitter of the fob. Upon receipt of a user name from the fob transmitter, the door generates a random pair of public-private keys and transmits the public key to the fob and the fob receiver without encryption. Hsu column 7, line 17-19. If the fob has validated the user's ID by matching the sensed fingerprint with reference image, the fob performs two levels of encryption on the fingerprint (CRC). The first encryption is with the door's public key. Then the CRC is encrypted using the fob's private key. Then the doubly encrypted CRC is transmitted to the door where it is decrypted. The process is graphically shown below.



Examiner acknowledges that Hsu does not show a comparison of finger print at the operator. See page 2 of Office Action bottom. Hsu scans the finger print at the fob and compares: A person 12 has fingerprint scanned and compared to a reference print at fob 14. A confirming message is sent to door 12.

Hsu also does not describe the transmission of constantly changing authorization codes. The authorization codes (the CRC values) in Hsu do not change. Rather they are encrypted using keys from the door where the door keys are changing with each transmission.

Hsu's discussion ***does not suggest a combining and a separating an always changing authorization signal combined signal as claimed.*** Hsu does not suggest combining codes,

transmitting a combined code and then separating the combined code at the operator as claimed. Hsu's authorization code never changes, but is encrypted. Applicants' authorization code always changes. Hsu's apparatus is complicated and requires a receiver and transmitter at the door. Hsu also requires a receiver at the transmitter outside the secured area. In short Hsu requires transreceivers at both the operator inside the secured area and at the finger print/reader on the fob outside the secured area. Hsu does not suggest the claims.

Flick

Flick is only concerned with finger print identification and it is this fingerprint identification that provides the required security.

Flick scans the finger print and sends only that fingerprint data --a vehicle start controller 86 receives biometric sensor data from remote transmitter 50. There can be a comparison at the transmitter or operator, but so-what. ***There is NO teaching of transmitter 50 sending a combined code which includes both a rolling code (which represents a particular transmitter) and finger print data.***

Flick does not suggest determining whether both fingerprint and rolling code are acceptable.

Flick does not suggest transmitting an always changing authorization code which is a combination the finger print with an access code and then splitting them.

Waraksa

Waraksa describes a passive keyless entry system. Transmitter 24 generates what the Examiner calls a rolling code, but this reference does not teach the use of both rolling code and fingerprint data or whether both are acceptable.

Waraksa does not teach combining a code representative of the finger print with an access code and then recognizing the access code and fingerprint code for access to a secure area. As can be seen by reference to column 8, lines 46 to 55 and column 10, lines 37 to 55,

Waraksa describes a clock for which a clock code is generated and which changes. This is not a rolling code, but this is not relevant because applicant acknowledges rolling code is known.

The references do not suggest using a changing combined authorization code which is a combination of a code representative of a fingerprint code and an ever changing rolling code

The Claims Are Non-Obvious In View Of The Applied Art Hsu, Flick and Waraksa

None of the references alone or in combination teach or suggest a system that determines the acceptance of an ever changing authorization code which is a combination of both a user fingerprint and a rolling code. Since elements of claim 1 are not taught or suggested by the prior art, it is believed that independent claims 1, 14 and 15 are allowable for this reason.

Hsu and Flick completely rely on the use of a signal representative of finger print data for entry into a secured area. Hsu requires a double encryption of a never changing CRC authorization code representative of a finger print and requires receipt of and the transmission of signals from the door and receipt of the signal from the door by the remote transmitter. Hence, while Hsu does to some extent protect against code grabbing biometric data, it does so in a complicated and expensive way.

The Commissioner is hereby authorized to charge any additional fees which may be required with respect to this communication, or credit any overpayment, to Deposit Account No. 06-1135.

Respectfully submitted,

FITCH, EVEN, TABIN & FLANNERY

Dated: October 20, 2008

Timothy E. Levstik
Registration No. 30,192

120 South LaSalle Street, Suite 1600
Chicago, Illinois 60603-3406
Telephone (312) 577-7000
Facsimile (312) 577-7007